UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH CALL NUMBER 404-863-7483 AND/OR IMEI: 310410349684800, THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	)	Case No. 1:21-mj-751

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A (incorporated by reference)

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Distribution of a Controlled Substance
21 U.S.C. § 846	Conspiracy to Distribute a Controlled Substance

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Brandon R. Cook

Applicant's signature

Brandon R. Cook, Task Force Officer DEA

Printed name and title

Sworn to before me and signed in my presence.
via FaceTime video

Date: October 21, 2021

Karen L. Litkovitz

Karen L. Litkovitz
United States Magistrate Judge

City and state: Cincinnati, Ohio

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with TELEPHONE NUMBER **404-863-7483** AND/OR **IMEI: 310410349684800** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account from August 1, 2021 to Present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

g. All records pertaining to the types of service used; and

h. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) and 865 those violations involving Steffen ROBERSON and occurring after August 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Evidence relating to the sale, purchase, and possession of illegal drugs, to include any preparatory steps taken in furtherance of the sale and possession of drugs;

(b) Evidence relating to the identity of co-conspirators and drug customers;

(c) Evidence related to the source of illegal drugs;

(d) Evidence of any communications with co-conspirators; evidence of any steps taken in furtherance of drug trafficking and evidence of any steps taken to conceal the possession of drugs;

(e) Evidence related to location of drug trafficking and storage of illegal drugs;

(f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(i) The identity of the person(s) who communicated with the user ID about matters relating to drug trafficking, including records that help reveal their whereabouts.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH TELEPHONE NUMBER 404-863-7483 AND/OR IMEI: 310410349684800 THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 1:21-mj-751 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Brandon R. Cook being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with [a] certain account[s] that [is/are] stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Police Officer with the Cincinnati (Ohio) Police Department, currently assigned as a Task Force Officer ("TFO") with the Drug Enforcement Administration ("DEA"). I have been assigned to the DEA since February 2021 and I have been a police officer for over 13 years, beginning in 2008. I earned a Bachelor of Arts Degree from Ohio State University in 2007. In 2008, I graduated from the Cincinnati Police Department's Police Academy and am certified as

a police officer through the Ohio Police Officer Training Academy (OPOTA). During the course of my law enforcement career, I have received hundreds of hours in various drug trainings, in addition to training in the use, preparation, and execution of search and seizure warrants. As a DEA TFO, my duties and responsibilities include conducting criminal investigations for violations of federal law, particularly those found in Title 21 and Title 18 of the United States Code. During my tenure as a Cincinnati Police Officer and with the DEA, I have participated in several criminal investigations seeking evidence of violations of the Controlled Substances Act (Title 21, of the United States Code).

3. The facts in this affidavit come from my personal observations, my training and experience, information from a confidential informant, and information obtained from other officers, agents, and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841(a)(1) and 846 have been committed by Steffan Roberson and other suspects known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The Cincinnati Police Department (CPD), the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and Hamilton County Regional Narcotics Unit (RENU) are investigating Steffan ROBERSON and his associates (hereinafter "the ROBERSON DTO") for drug trafficking in the Cincinnati, Ohio area.

A. A reliable confidential information identified Alton BEACHER as a methamphetamine trafficker in the Cincinnati area.

7. During the week of August 29, 2021,[1] CPD narcotics Detective Jonce Tackett met with a confidential informant (CI-1)[2], who stated an individual known to him/her as "Yo" is trafficking methamphetamine. CI-1 told investigators that "Yo" is involved in the sale of methamphetamine in the greater Cincinnati area and uses the telephone number (419) 936-0005 to coordinate methamphetamine sales with customers and co-conspirators. CI-1 is reliable and has provided information on this case and others that law enforcement independently verified as true and correct. Additionally, as explained below, information provided by CI-1 has been corroborated through controlled purchases of drugs made at the direction of law enforcement. CI-1 can identify marijuana, heroin, methamphetamine, and cocaine due to past contacts with the drug as well as association with drug users and illegal drug traffickers.

8. During the meeting, CI-1 stated "Yo" is a male black who uses the Instagram account, "Frank_Castilla16." Through law enforcement databases, officers identified the user of Instagram account, "Frank_Castilla16," as Alton BEACHER. Detective Tackett showed CI-1 a current Ohio BMV photo of BEACHER and CI-1 positive identified BEACHER as the person CI-

[1] The exact date of the meeting is known to law enforcement, but omitted to protect the identify of CI-1.

[2] CI-1 has previous convictions for Weapons Under Disability and Trafficking in Drugs. CI-1 is currently cooperating for case consideration.

1 knows as "Yo". Additionally, CI-1 advised that BEACHER sells methamphetamine out of an apartment inside the multi-family building located at 1441 Hillcrest Road, Cincinnati, Ohio.

9. After CI-1 identified BEACHER as the drug trafficker CI-1 knew as "Yo," I searched Hamilton County, Ohio Clerk of Court records and learned BEACHER has the following felony convictions: two convictions for Having Weapons Under Disability (Case Numbers B0908743 and B1801428); Trafficking in Heroin (Case Number B1000459); Trafficking in Cocaine (Case Number B0500078); two convictions for Possession of Cocaine (Case Numbers B050078 and B0411790); and Trafficking in Drugs (Case Number B0311908).

B. BEACHER and members of the ROBERSON DTO sold CI-1 methamphetamine during a controlled drug buy.

10. Between August 30 and September 1, 2021,[3] law enforcement met with CI-1 to conduct a recorded and controlled methamphetamine purchase from BEACHER using CI-1. Prior to the controlled purchase, law enforcement searched CI-1 and the CI-1's vehicle for contraband and U.S. Currency with nothing found. Detective Tackett directed CI-1 to place a one-party, consensually recorded phone call to BEACHER on cellular telephone number (419) 936-0005 (hereinafter "BEACHER Phone 1"). During the conversation, BEACHER told CI-1 to go to "the spot" and that "Smoke" will provide CI-1 with the methamphetamine. CI-1 knew "the spot" to mean the apartment located at 1441 Hillcrest Road. While under the constant monitoring and control of Detective Tackett, CI-1 traveled to 1441 Hillcrest Road. CI-1 entered the common entry door for 1441 Hillcrest Road, walked up one flight of stairs, and entered the door to the right at the top of the first flight of steps. CI-1 was let inside and met by "Smoke." CI-1 gave "Smoke" the pre-recorded U.S. Currency, and in exchange, "Smoke" gave CI-1 methamphetamine. While inside the apartment, CI-1 spoke with another individual known to him/her as "Worm." "Worm"

[3] The exact date of the controlled purchase is known to law enforcement but omitted to protect the identity of CI-1.

offered to sell CI-1 cocaine. CI-1 then left 1441 Hillcrest and traveled to a neutral location while under constant monitoring and control by law enforcement. Investigators met with CI-1 where CI-1 immediately surrendered methamphetamine and the digital recording device. Investigators searched CI-1 and CI-1's vehicle for contraband and U.S/ Currency with nothing found.

11. During a debriefing, CI-1 confirmed "Smoke" provided him/her with the methamphetamine. Based on experience, investigators are familiar with a male black who goes by the street name "Smoke" and know him as Quinton JENNINGS. Investigators showed CI-1 a recent Ohio BMV photo of JENNINGS and CI-1 positively identified JENNINGS as the person CI-1 knows as "Smoke."

12. Detective Tackett searched Hamilton County, Ohio Clerk of Courts records and learned JENNINGS has previously been convicted of the following felonies: Robbery (Case Number B0005014); Trafficking in Heroin (Case Number B1300414); and Possession of Heroin (Case Number B1306159).

13. From previous drug trafficking investigations, investigators are familiar with Steffen ROBERSON, who goes by the street name "Worm." Investigators showed CI-1 a recent Ohio BMV photo of ROBERSON. CI-1 positively identified ROBERSON as the person CI-1 knows as "Worm" who offered to sell CI-1 cocaine during the controlled drug buy.

14. Detective Tackett searched Hamilton County, Ohio Clerk of Courts records and learned that ROBERSON has the following felony convictions: Possession of Cocaine (Case Number B0106593); Tampering with Evidence (Case Number B016593); Possession of Marijuana (B0908441); Possession of Heroin (B1205458); and Trafficking in Cocaine (B0501423).

15. Detective Tackett reviewed the lawfully recorded audio/video of the controlled buy and from JENNINGS and ROBERSON. The audio/video of the controlled buy corroborated the information provided by CI-1.

C. In the past, JENNINGS worked for the ROBERSON DTO and acts on behalf of and at the direction of ROBERSON.

16. I know, from previous investigations, as well as reporting from confidential sources of information, that JENNINGS and ROBERSON are close associates. Historical information provided by cooperating informants to RENU, FBI, and CPD, including CI-1 and later identified CI-2, state that ROBERSON directs JENNINGS and other members of the ROBERSON DTO. CI-1 stated the cocaine, marijuana, and fentanyl sold by JENNINGS and others are ROBERSON's drugs. Additionally, other sources of information provided historical information that, in the past, JENNINGS has been ROBERSON's top trusted co-conspirator and often facilitates all transactions with illegal drugs on behalf of ROBERSON.

D. ROBERSON is using phone number (404) 863-7483 to via FaceTime with JENNINGS.

17. On September 2, 2021, investigators directed CI-1 to place a one-party consensually recorded FaceTime call to JENNINGS at phone number (513) 430-6338 (hereinafter "Jennings Phone 1"). During the FaceTime call with JENNINGS, CI-1 asked JENNINGS about the cocaine ROBERSON offered to sell CI-1. JENNINGS stated he had to call ROBERSON to see if he's at the "spot" (1441 Hillcrest Road). CI-1 attempted to call JENNINGS again on Jennings Phone 1, but JENNINGS did not answer.

18. After the September 2, 2021 FaceTime call, investigators obtained a search warrant for JENNING's Apple iCloud account. Investigators reviewed the September 2, 2021, FaceTime call log for Jennings Phone 1. The FaceTime call log showed after JENNINGS received a FaceTime call from CI-1, JENNINGS placed a FaceTime call to an unidentified telephone number, then to co-conspirator BEACHER on Beacher Phone 1, and then placed FaceTime call to **(404) 863-7483 (Roberson Phone 1**). Within 45 minutes of the initial phone call to Jennings Phone 1, JENNINGS placed a call to **Roberson Phone 1**. I know the 404-area code is an Atlanta, Georgia

area code. Additionally, review of JENNINGS' iCloud account showed JENNINGS regularly communicated with **Roberson Phone 1** using FaceTime.

19. Investigators searched law enforcement databases for ROBERSON and learned ROBERSON had a recent address in Atlanta, Georgia at 889 Lenox Court NE, Atlanta, Georgia 30324. Additionally, federal agents executed a lawful search warrant at Steffen ROBERSON's address in December 2019 at 270 17th Street NW, Atlanta, Georgia.

20. DEA agents subpoenaed historical toll records for **Roberson Phone 1**. On September 23, 2021, agents received the historical tolls records and reviewed the top incoming and outgoing calls for **(404) 863-7483, Roberson Phone 1**. Multiple illegal drug traffickers known to be associated to ROBERSON and the ROBERSON DTO were in the top callers for **Roberson Phone 1** including ROBERSON's brother, Anthony Roberson at (513) 658-5828, Sterling PARISH[4] at (513) 886-1156, and co-conspirators JENNINGS at Jennings' Phone 1, and BEACHER at Beacher Phone 1.

21. Detective Tackett shared Roberson Phone 1, believed to be Steffen ROBERSON's telephone number, with FBI Agent Tony Ott. Agent Ott stated **Roberson Phone 1** has been in contact with individuals the FBI has identified within the ROBERSON DTO including Shawn BARTON at (513) 713-9877, Ronald BARNETT at (513) 485-1590, and Jerome NEWTON at (513) 212-4493.

22. On October 5, 2021, Hamilton County Common Pleas Judge Tom Heekin authorized a search warrant for historical records and electronic surveillance of **Roberson Phone 1**. Information lawfully obtained pursuant to this search warrant included subscriber information,

[4] In 2018, FBI agents recovered distribution quantity of fentanyl from Anthony Roberson during the execution of a search warrant and distribution quantity of fentanyl from Parish during a vehicle pursuit.

call history, tower locations, and 30 days of Real Time Precision GPS Tracking (Ping) data collection for **Roberson Phone 1**.

23. On October 6, 2021, investigators reviewed the GPS data for **Roberson Phone 1** and learned the handheld device was in a 98-meter ping radius in the Northside neighborhood of Cincinnati, Ohio and had been so since the previous evening. Through investigation and vehicle tracker information, investigators were familiar with a house at the corner of William P Dooley Bypass and Old Ludlow Avenue that Quinton JENNINGS frequented. The GPS Phone Ping radius shows the intersection of William P Dooley Bypass and Old Ludlow Avenue. Surveillance officers drove to the area and saw a white 2018 Honda Accord bearing Texas temporary tag 28680K5, which was registered to a Steffen ROBERSON of 6028 Lantana Avenue Cincinnati, Ohio 45224. The 2018 Honda was parked in front of 3920 Old Ludlow Avenue near the location JENNINGS had previously frequented.

24. At 10:10 a.m., surveillance officers saw a heavy set male black exit 3920 Old Ludlow Avenue, get into the driver seat of the white 2018 Honda Accord, and drive away. The GPS Phone Ping from **Roberson Phone 1** remained in the area when white 2018 Honda Accord returned back to 3920 Old Ludlow at 10:18 a.m. It should be noted the GPS Phone Ping for **Roberson Phone 1** stayed at the address 3920 Old Ludlow while the vehicle was gone. I believe, based on my training and experience, that ROBERSON stayed at Old Ludlow while the heavy set male black was gone from the location.

25. At 11:50 a.m., surveillance officers saw a male black matching the physical description of ROBERSON exit 3920 Old Ludlow Avenue. ROBERSON waved to a silver Nissan Altima bearing Ohio passenger plate JEJ6092 registered to a Tremar Roberson of 4028 Ledgewood Drive, which was parked on Old Ludlow Ave. The silver Nissan pulled forward and the male black believed to be ROBERSON conducted a hand-to-hand transaction with a female black in the silver Nissan exchanging what surveillance officers believed to be marijuana for U.S. Currency.

26. At 4:46 p.m. that same day, investigators reviewed the GPS Phone Ping for **Roberson Phone 1**, and the GPS Ping radius showed the handheld device was within 134 meters of the intersection of Trapp Lane and Trapp Court in the City of Mount Healthy. Investigators are familiar with ROBERSON's mother, Wanda Roberson, who lives at 10046 Trapp Lane Cincinnati, Ohio 45231. Wanda Roberson's residence, 10046 Trapp Lane, is within 134 meters of the center of the GPS Phone ping for Roberson Phone 1. Therefore, I believe that ROBERSON was using **Roberson Phone 1** and was at his mother's residence.

27. At approximately 8:07 p.m., **Roberson Phone 1** started traveling west bound on I-275 and arrived near the Hollywood Casino in Lawrenceburg, Indiana at approximately 8:22 p.m.

28. The following day, October 7, 2021, investigators met with the Casino Gaming Agents for Hollywood Casino in Lawrenceburg, Indiana. The Gaming Agents along with investigators reviewed camera footage from October 6, 2021 and identified Steffen ROBERSON entering the Hollywood Casino at 8:24 p.m., shortly after the GPS Phone Ping for **Roberson Phone 1** arrived near the Hollywood Casino. The heavy-set male on video with ROBERSON was the same male who surveillance officers saw get into the white Honda Accord during the morning of October 6, 2021. He was subsequently identified as Charles Lee[5] by a confidential and reliable informant.

29. On October 7, 2021, Detective Tackett reviewed the GPS Phone Ping data for **Roberson Phone 1** and learned at 1:30 p.m., **Roberson Phone 1** was near Hollywood Casino in Lawrenceburg, Indiana. Surveillance officers drove to the Hollywood Casino and saw the white 2018 Honda registered to ROBERSON (hereinafter "Target Vehicle") parked in the parking

[5] Detective Tackett searched Hamilton County Clerk of Courts records and learned Charles Lee has the following felony convictions: two convictions for Trafficking in Heroin (Case Numbers B1304328 and B1705380); Trafficking in Cocaine (Case Number B0504489); and Possession of Heroin (Case Number B1304328); Possession of Cocaine (Case Number B0507080); two convictions for Having Weapons Under Disability (Case Numbers B1801802 and B0704264); and Permitting Drug Abuse (Case Number B1801802).

garage. Surveillance officers went inside the casino and saw Charles Lee and another male black matching the physical description of ROBERSON, but was wearing a face mask, while inside the casino. Surveillance officers continued watching the Target Vehicle and at approximately 2:40 p.m., Lee and the male black believed to be ROBERSON got into the Target Vehicle and left the casino. At 2:46 p.m., the GPS Phone Ping indicated **Roberson Phone 1** had left the casino and was moving with the Target Vehicle. Surveillance officers followed the Target Vehicle, which was driving 5 to 10 miles an hour under the speed limit while traveling on I-275 East. Based on my training and experience, I know illegal drug traffickers will often drive under the speed limit to identify law enforcement vehicle who are attempting to follow their vehicles. I also know, based on my training and experience, that drug traffickers will drive in this manner before or after they are travel to a secure location where drugs and proceeds of drug trafficking are stored.

30. Surveillance officers maintained a visual of the Target Vehicle and followed the Target Vehicle as it traveled to the City of Mount Healthy. Surveillance officers saw the Target Vehicle pull into the driveway of a single-family home located at 7216 Park Avenue, Mount Healthy, Ohio 45231. Throughout surveillance **Roberson Phone 1** moved with the Target Vehicle.

31. Based on my training and experience, as well as the investigation in this case, I believe ROBERSON is using **Roberson Phone 1** and the Apple iCloud Account associated with **Roberson Phone 1** (**SUBJECT ACCOUNT**). My belief is based on the fact that after CI-1 asked JENNINGS about buying cocaine from ROBERSON, JENNINGS placed a FaceTime call to **Roberson Phone 1**. I know that **Roberson Phone 1** has an Atlanta area code and ROBERSON previously lived in Atlanta. My belief is further based on the fact that physical surveillance of ROBERSON and GPS Phone Ping data for **Roberson Phone 1** showed that **Roberson Phone 1** moved with ROBERSON. I further believe ROBERSON is using the **SUBJECT ACCOUNT** in furtherance of his drug trafficking activities. This belief is based on my review of toll records for **Roberson Phone 1**, which shows multiple calls with known drug traffickers in the ROBERSON

DTO. JENNINGS' iCloud account, which shows that JENNINGS had multiple FaceTime calls with the **SUBJECT ACCOUNT** and I know FaceTime is a service exclusive to Apple users. I also know, based on my training and experience, that drug traffickers use FaceTime calls to evade law enforcement detection.

BACKGROUND CONCERNING APPLE[6]

32. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

33. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-

---

[6] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

34. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

35. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

36. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs"

for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

37. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

38. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party

apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

39. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

40. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

41. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

42. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

43. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. For example, I know based on my training and experience, that drug traffickers use various financial apps to transfer money. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

44. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

45. Based on the forgoing, I request that the Court issue the proposed search warrant.

46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

47. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Brandon R. Cook

BRANDON COOK
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me on October 21, 2021.

Karen L. Litkovitz

Karen L. Litkovitz
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with TELEPHONE NUMBER **404-863-7483** AND/OR **IMEI: 310410349684800** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account from August 1, 2021 to Present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

g. All records pertaining to the types of service used; and

h. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) and 865 those violations involving Steffen ROBERSON and occurring after August 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Evidence relating to the sale, purchase, and possession of illegal drugs, to include any preparatory steps taken in furtherance of the sale and possession of drugs;

(b) Evidence relating to the identity of co-conspirators and drug customers;

(c) Evidence related to the source of illegal drugs;

(d) Evidence of any communications with co-conspirators; evidence of any steps taken in furtherance of drug trafficking and evidence of any steps taken to conceal the possession of drugs;

(e) Evidence related to location of drug trafficking and storage of illegal drugs;

(f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(i) The identity of the person(s) who communicated with the user ID about matters relating to drug trafficking, including records that help reveal their whereabouts.